(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－326256

(43)公開日　平成10年(1998)12月８日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ａ
	13/00	３５１		13/00	３５１Ｚ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７１
	9/36				６８５
	12/28			11/00	３１０Ｚ

審査請求　未請求　請求項の数10　ＦＤ　（全 12 頁）　最終頁に続く

(21)出願番号　特願平9－364061

(22)出願日　平成９年(1997)12月17日

(31)優先権主張番号　０８／７６９６０３

(32)優先日　1996年12月18日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　591064003
サン・マイクロシステムズ・インコーポレーテッド
SUN MICROSYSTEMS, INCORPORATED
アメリカ合衆国　94303　カリフォルニア州・パロ　アルト・サン　アントニオ　ロード・901

(72)発明者　ガリー・ダブリュ・ウィニガー
アメリカ合衆国　94040　カリフォルニア州　マウンテンビュー　サンモアアベニュー　2379

(74)代理人　弁理士　遠藤　恭

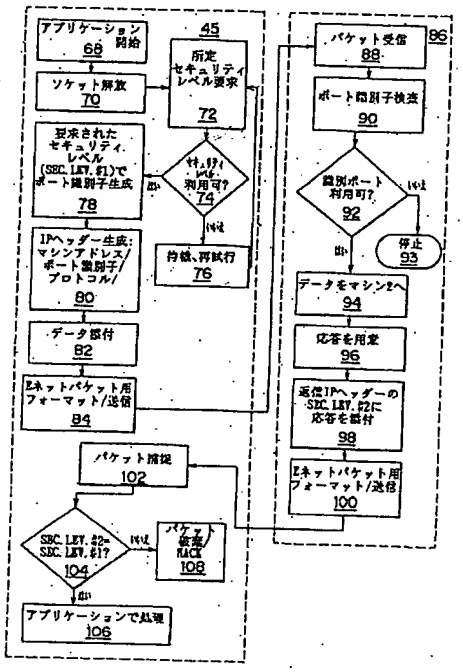
最終頁に続く

(54)【発明の名称】　マルチレベルセキュリティポート方法、装置、及びコンピュータプログラム製品

(57)【要約】

【課題】　セキュリティポリシーの要求を満しつつ、同じポート番号を有する複数のソケットを同時に開放させ、サードパーティアプリケーションがセキュリティポリシーによって妨げられないかのようにそれらを実行させるマルチレベルオペレーティングシステムの下で作動するコンピュータ上のマルチポートシステム及び方法を提供する。

【解決手段】アクセス制御セキュリティ機構に従うオペレーティングシステムを有するコンピュータシステム。本システムは、セキュリティ分類レベルの階層が定義されている政府の及び商用のシステムを含む。アクセス制御セキュリティ機構による秘密度ラベルは、少なくとも階層型のセキュリティ分類を含み、システム内の情報の個別領域を表現する階層的でないカテゴリー又は区分を含んでよい。ポートは、ポート番号及び秘密度ラベルによって特徴づけられ、同一ポート番号の固有の秘密度ラベルを有する複数のポートを開放することを可能にする。



1

【特許請求の範囲】

【請求項１】　一つの共通ポート番号に関連付けられた複数のポートであって、該各ポートがそれぞれ選択された秘密度ラベルを有し、前記ポート番号と前記秘密度ラベルが少なくとも一つの前記ポートのポート識別子を特定するもの、を生成し、前記ポートに対する多重同時アクセスを可能にするコンピュータ読み取り可能プログラムコード機構を有するコンピュータ使用可能媒体を備えるコンピュータプログラム製品であって、前記コンピュータ読み取り可能プログラムコード機構が、

プロトコルヘッダーを備える通信パケットを構成する第１のコンピュータ読み取り可能コード機構であって、前記プロトコルヘッダーが、少なくとも発信元マシン識別子、発信元ポート番号、及び宛先ポート番号と秘密度ラベル領域を含む宛先ポート識別子領域とを備えるものと、

受信側ポートを確立するために通信パケットの受信を許可する第２のコンピュータ読み取り読み取り可能コード機構と、を含むコンピュータプログラム製品。

【請求項２】　マシンで実行可能な命令群のプログラムを備え、マルチレベル信頼システムにおいて資源の多重同時アクセスを可能にするマルチレベルポートを確立するマシン読み取り可能な第１のプログラム記憶装置であって、

第１のプロセスでインスタンス化されたアプリケーションが起動されている発信元マシンから、少なくとも第１の宛先ポート番号と第１の秘密度ラベルとを備えた通信パケットを受信するように構成された第１のコンピュータ読み取り可能コード機構と、

ポート識別子を提供する前記ポート番号と前記秘密度ラベルを識別するために前記パケットを検査するように構成された第２のコンピュータ読み取り可能コード機構と、

前記ポート識別子を、既に開放されているポートに関連付けられたポート識別子と比較するように構成された第３のコンピュータ読み取り可能コード機構と、

前記ポート識別子の秘密度ラベルが、既に開放されているポートの秘密度ラベルと比較して固有のものである場合、該既に開放されているポートと同じポート番号を有するポートを開放し、同じポート番号、固有の秘密度ラベルを有する複数のポートについての同時プロセスを可能とするように構成された第４のコンピュータ読み取り可能コード機構と、を含む第１のプログラム記憶装置。

【請求項３】　前記第３及び第４のコンピュータ読み取り可能コード機構を含むセキュリティ部を有するカーネルをさらに含む請求項２記載の第１のプログラム記憶装置。

【請求項４】　請求項３記載の第１のプログラム記憶装置において、

前記通信パケットのデータ部分を、前記ポートを開放するステップで開放されたポートに関連付けられたアプリケーションをインスタンス化するプロセスに引き渡すように構成された第５のコンピュータ読み取り可能コード機構と、

少なくとも宛先ポート番号、第２の秘密度ラベル、及び応答を含む応答通信パケットを、前記第１のプロセスへ伝送するために準備するように構成された第６のコンピュータ読み取り可能コード機構と、

前記応答通信パケットを前記発信元マシンへ伝送するように構成された第７のコンピュータ読み取り可能コード機構と、

前記発信元マシンのセキュリティプロトコルに従って、前記発信元マシンにより前記応答通信パケットを処理するように構成された第８のコンピュータ読み取り可能コード機構と、をさらに含む第１のプログラム記憶装置。

【請求項５】　マルチレベル信頼オペレーティングシステムを有するコンピュータにおいて、

一つの共通ポート番号に関連付けられた複数のポートであって、該各ポートがそれぞれ固有の秘密度ラベルを有し、前記ポート番号と前記秘密度ラベルの組み合わせが前記各ポートの固有のポート識別子を特定するもの、を生成し、該複数のポートが前記共通ポート番号の多重同時アクセスを可能にするコンピュータ読み取り可能プログラムコード機構を有するコンピュータ使用可能媒体を含むコンピュータ。

【請求項６】　前記コンピュータ読み取り可能コード機構が、さらに通信パケットを受信し、宛先ポート番号と秘密度ラベルを抽出するため前記パケットを検査し、固有のポート識別子アドレスを有するポートの空きを判断し、固有のポート識別子アドレスを有するポートを開放するコンピュータ読み取り可能コード手段を含む請求項５記載のコンピュータ。

【請求項７】　複数のプロセスによる同時アクセスを可能にするマルチレベルポートであって、各プロセスが異なる秘密度ラベルを有し、前記マルチレベルポートが共通のポート番号と複数の選択された固有の秘密度ラベルによって特定され、同じ秘密度ラベルを持った複数のプロセスとポートとの間の双方向通信を可能にするマルチレベルポート。

【請求項８】　マルチレベル信頼システムで複数のプロセスにより一つのポートの同時アクセスを可能にする方法であって、

第１のコンピュータシステムのカーネルにより生成され、宛先ポート番号及び第１の秘密度ラベルを備えた通信パケットを、第２のコンピュータシステムで捕捉するステップと、

その組み合わせがポート識別子を特定する前記ポート番号及び前記秘密度ラベルを抽出し、識別するため前記通信パケットを検査するステップと、

前記ポート識別子を、既に開かれているポートのポート

番号及び秘密度ラベルと比較するステップと、
前記通信パケットで特定されるのと同じポート識別子を有する既に開かれているポートが無い場合に、ポートを確立するステップと、
前記通信パケットを、前記ポート識別子と等しいポート番号及び秘密度ラベルを有する前記第２のコンピュータシステムのアプリケーションプロセスに引き渡すステップと、を含む方法。

【請求項９】　一つのポートの同時アクセスを可能にする請求項８記載の方法において、
応答を準備するステップと、
少なくとも応答、発信元ポート番号、及び前記第２のコンピュータシステムの前記アプリケーションプロセスに関連付けられた第２の秘密度ラベルを備えた第２の返信通信パケットを生成するステップと、
前記第２の通信パケットを、前記第１のコンピュータシステムへ送信するステップと、
前記第１のコンピュータシステムのカーネルにより、前記第２の通信パケットを捕捉するステップと、
前記第１の秘密度ラベルを前記第２の秘密度ラベルと比較するステップと、
前記第１のコンピュータシステムの前記カーネルに関連付けられたセキュリティプロトコルに従って前記応答を処理するステップと、をさらに含む方法。

【請求項１０】　一つのポートの同時アクセスを可能にする請求項８記載の方法において、前記捕捉ステップが、OSIプロトコル下で動作する第２のコンピュータシステムのデータリンク層とネットワーク層との間で作動するデーモンによって実行される方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータシステムで動作可能なマルチレベルポート方法、装置及びコンピュータプログラム製品に関し、より詳細には、マルチレベルの多層セキュリティレベルを利用したマルチレベルオペレーティング・システムで動作可能なマルチレベルポートシステムに関するものである。

【０００２】

【従来の技術】機密性のあるコンピュータシステムでは、許可を得ずに情報を開示することが制限されている。政府のセキュリティシステムは、情報に対するユーザーによるアクセスを所定のセキュリティ基準に従うものに限って許可する。その他のセキュリティ環境では、給与支払い表、社内の覚書や競争的戦略文書を含むその他の機密企業データを含む特定のプライベート情報が保護される。

【０００３】政府または企業のシステムに対してコンピュータの機密性を確立するためには、セキュリティポリシーが採用される。セキュリティポリシーは、機密情報の管理、保護及び配布のためのルールを確立する。セキュリティポリシーは通常、サブジェクト(subject)とオブジェクト(object)と言う言葉を使って記述される。サブジェクトは、選択されたシステム内でアクティブになり、例えば、ユーザー、プロセス及びプログラムを含む。オブジェクトはサブジェクトのアクションを受け取るものであって、ファイル、ディレクトリ、デバイス、ソケット及びウィンドウのようなものである。セキュリティポリシーは、サブジェクトのユーザーが、ファイルのような特定のオブジェクトに対してアクセスできるかどうかを決定するルールを定めることができる。

【０００４】David BellとLeonard Lapadulaによって1973年に開発された周知のセキュリティシステムには、メッセージ作成プロセスのセキュリティ基準に従うアクセスルールを持ったマルチレベル機密コンピュータシステムが記載されている。アクセスルールを基にしたセキュリティシステムは、システムのサブジェクトとオブジェクトの間の許可されたアクセス関係を強化する参照モニター(reference monitors)に依存する。Roger Shellが1972年に開発したセキュリティカーネルのコンセプトは参照モニター概念を実装し、システムのすべての活動がシステムのセキュリティポリシーにしたがって管理される、したがって、カーネルは仲介を行なう。「信頼されるシステム」は、ハードウェアとソフトウェアの十分な統一性を持ち、アクセス特権に抵触せずに多様な組み合わせのユーザーに対して、ある領域の秘密扱い又は秘密扱いでないセキュリティ情報を同時的に使用することを可能にする。

【０００５】ネットワークでは、信頼されるシステムのセキュリティ機構が、信頼されるシステムとの通信を制御できることが要求される。従来では、ネットワーク管理機能は、システムの他のシステムとの接続に対して通常厳格な制御を行なってきた。しかしながら、相互に接続されたネットワークと、容易な遠隔アクセスと、資源のシェアリングが一般的になるにつれて、システムがネットワーク全体を識別または信頼できないことがしばしば起きるようになった。

【０００６】ネットワーク環境の中で機密性を確立する戦略は、所定のセキュリティ属性または秘密度ラベル(sensitivity labels)、情報ラベルを持つラベル添付データを必要とする。これにより、あるネットワークの他のシステムでデータの機密性の認証が可能となる。異なるネットワークは異なるセキュリティポリシーをサポートするため、これらのラベルは必ずしも同じフォーマットによるものではない。ある機密ネットワークでは、各システムが異なる種類のラベルを持つことができる。ユーザーの秘密度ラベルは、そのユーザーに関連付けられた秘密度レベル、または信頼のレベルを示す。同様に、ファイルの秘密度ラベルは、ユーザーが特定のファイルにアクセスできなければならないという信頼のレベルを示す。強制的なアクセス制御は、誰がシステム内のどの情

報にアクセスできるかを決定する秘密度ラベルの使用を制御する。ラベル添付と強制アクセス制御は、互いに、単独のコンピュータシステム内の多数の異なるセキュリティレベルにおける多数の情報分類を取扱うポリシーである、マルチレベルセキュリティポリシーを実装する。

【０００７】強制的アクセス制御の下では、強制アクセス制御をサポートするシステム内の一つ一つのサブジェクトとオブジェクトは、それと関連付けられた秘密度ラベルを保持している。一つの秘密度ラベルは一般的に、一つの分類と一組のカテゴリーまたは区画を有する。この分類システムは通常階層的であり、例えば軍のセキュリティモデルでは、トップシークレット、シークレット、コンフィデンシャル及びクラシファイドのような多層識別レベルを含む。企業環境においては、カンパニコンフィデンシャルまたはカンパニプライベートのようなラベルを含む、他の分類を使うことができる。

【０００８】通常、サブジェクトがオブジェクトを読み取るためには、そのサブジェクトの秘密度レベルは、オブジェクトの秘密度レベルに対して支配的でなければならない。サブジェクトの秘密度ラベルは、もしそのサブジェクトの分類が、そのオブジェクトの分類と等しいか、それよりも高ければ、そのオブジェクトの秘密度ラベルを支配する。同様に、一つのオブジェクトを書き込むためには、そのオブジェクトの秘密度レベルは、そのサブジェクトの秘密度レベルを支配しなければならない。サブジェクトがオブジェクトに書き込みするためには、そのサブジェクトの秘密度レベルは、そのオブジェクトまたはファイルの秘密度レベルと等しいかそれよりも高くなければならない。したがって、現状の強制アクセスシステムにおいては、サブジェクトがオブジェクトに対して自由に書き込みと読み取りを行なうためには、そのサブジェクトとオブジェクト両方が同じ分類レベルを持たなければならない。これは、アクセス制御システムが働き、また信頼されるコンピュータシステムの間で双方向の通信を行なうことができるための基本的なルールである。

【０００９】

【発明が解決しようとする課題】現在のネットワーク化されたマルチレベル信頼システムにおいて、サードパーティアプリケーションは、効果的に動作するための十分なサポートを持たない。特に、異なる秘密度ラベルを持つ多数のプロセスが、セキュリティレベルの違いを越えて、同じオブジェクトまたは資源にアクセスしようとするとき、その動作が停止することがある。図１の先行技術のダイアグラムでは、一つのアプリケーションが、一つの信頼されるシステムの上を走り、ネットワーク上の同じシステムまたは別のシステム上の資源(即ち、ファイル、アプリケーションまたはデータベース)にアクセスを試みている。この試みが成功する、つまり該当するアクセス制御セキュリティ機構にしたがって双方向の通信ができるためには、資源とサブジェクトのセキュリティレベルは、同一でなければならない。

【００１０】図１において図式的に示されるように、先行技術のマルチレベル信頼システムにおいては、ある特定の秘密度レベル上を走るプロセス(サブジェクト)による資源またはサービス(オブジェクト)へのアクセスは、アクセス制御メカニズムによって強制されているため、要求するプロセスと同一の秘密度レベルを持つメモリー内のオブジェクトに制限される。したがって、双方向通信は、そのサブジェクトとオブジェクトが異なる秘密度レベルを持っている場合には排除される。呼び出されたアプリケーション、サービスまたは資源がコンピュータのメモリー内で一旦インスタンス化されると、そのプロセス、サービスまたは資源に秘密度レベルが関連付けられ、同様にその資源へのアクセスを希望するが、しかし異なるクリアランスを持つアプリケーションを走らせている他のプロセスによるアクセスは、否定される。

【００１１】しかしながら、以下に記述される図２の先行技術のシステムにおいては、ある受信システム上のあるポートが特定のセキュリティ分類、クリアランスレベルまたは秘密度ラベルにおいて、ある実質的な時間間隔だけ解放されたままでいると、別の技術的問題が発生する。これは、あるポートが既に開かれ、ある異なるクリアランスの下で解放されたままであるとき、異なるクリアランスを持つユーザーまたはシステムがその同じ資源にアクセスするのを阻害する。ポート番号は、アクセスされる資源または第三者のシステムに固有のものであるため、その特定のポートが得られないと、異なるクリアランスを持つ他のユーザーまたはシステムがその第三者の資源にアクセスするのを実質的に排除する。これは、異なるセキュリティレベルで動作するアプリケーションに対して、その資源を実質的に利用できないようにする。

【００１２】したがって、システムや方法に対して、多様なセキュリティレベルで動作する資源へのアクセスができるようにする必要がある。そのようなシステムや方法は、異なるセキュリティ分類レベルを持つプロセスに対して透過的でなければならない。

【００１３】現状のマルチレベル信頼システムでのさらなる問題は、関連するシステムポートまたはコバート通信路(covert channel)の間のレベル間信号チャンネル通信からのセキュリティの侵害である。コバート通信路は、システム内の通信では通常使われず、したがってそのシステムの正規のセキュリティ機構で保護されていない、情報経路である。そのため、セキュリティプロトコルを侵すことによって他の人またはプログラムに情報を通信する秘密の方法がある。コバート通信路は、データ属性の変化またはシステムの性能またはタイミングの変化によって情報を伝達する。格納データ及びシステムのタイミングに対する属性の変化をモニターすることによ

って、秘密情報を推断することができる。メッセージ長、頻度及び宛先のようなデータ特性は、コバート通信路分析、メッセージの実際の特性を偽るためにパッドを付けることあるいは、ノイズや偽のメッセージを送信するような技術を使うことによって、侵入者によるデータ交信の分析や、同一のシステム上で低位の分類を持つユーザーから保護できる。しかしながら、これらの手段は、データのセキュリティを保証しない。

【００１４】したがって、セキュリティプロトコルに侵入して、多機密レベルコンピュータシステム内で統治された分類を持つポートへのデータアクセスを防止する必要がある。そのようなシステムや方法は、属性情報を侵入者へ引き渡すことを防ぐための統治されたポートのアクセスを確保しなければならない。

【００１５】

【課題を解決するための手段】本発明によれば、マルチレベル信頼システムは、多ポートの端点(endpoints)を単独の識別コード表示または名前と関連付ける。多ポート端点と関連付けるために単独の識別方法を使うことにより、端点がさらに共通の識別コード表示と関連付けられる場合には、端点間の通信を停止するセキュリティチェックを設けることが可能となる。これは、レベル間通信に起因するセキュリティに対する危険を減少させるために有益である。

【００１６】本発明によれば、選択されたネットワークレベルにおける第三者の通信のために特権を行使することは、多指定レベルに対して肯定的に与えられる。これは、それにより希望するマルチレベルでのアプリケーションの使用を直接かつ修正なしで行なえるため、アプリケーションソフトの修正なしにマルチレベル信頼システムを動作させられる利点がある。

【００１７】本発明によれば、コンピュータシステムは、マルチレベル信頼システムにおいて、多重の、実質的に同時的な資源へのアクセスを可能にするマルチレベルポートを確立するための方法を実現するマシンにより実行可能な命令群のプログラムを含む、マシンにより読み取り可能なプログラム格納装置で構成される。

【００１８】本発明によれば、コンピュータシステムは、マシンアドレスと固有のポート識別子を持つ宛先ソケットを含むインターネットプロトコル(IP)ヘッダーで構成されるオブジェクトアクセスパケットを生成するためのマルチレベルアクセス制御セキュリティ機構を支援するオペレーティングシステムカーネルと、資源またはオブジェクトを指定するポート番号を含むポート識別子と、アクセス制御セキュリティプロトコルのための秘密度ラベルとで構成される。本発明によれば、選択された固有の秘密度ラベルにおける単独の選択されたポート番号に対して、一つの宛先システム上に複数のプロセスが生成され、そのため多様なユーザーがマルチレベルアクセス制御システムにおいて、選択されたセキュリティポリシーにしたがって、選択されたポートにおける資源やオブジェクトにアクセスできるようになる。

【００１９】本発明の方法によれば、マシン読み取り可能コードは、選択されたアプリケーションの同じポートアドレスと異なる秘密度ラベルを持つ複数のインスタンスを開く。

【００２０】本発明によれば、同じポート番号であるが、別のセキュリティ分類ラベルを持つマルチネットワーク端点が確立され、そのため、依然としてそのシステムのセキュリティポリシーに準じながら、共通のポート番号による同時的なプロセスポートへのアクセスが可能となる。システムアクセス制御セキュリティプロトコルによって使われる異なるセキュリティ分類の数と同じ数のポートをその同じポート番号で開くことができる。

【００２１】

【発明の実施の形態】図２は、アクセス制御セキュリティ機構を採用した先行技術システムのフロー図である。サードパーティアプリケーションは、遠隔の第三者コンピュータシステムからのライセンスの認証を必要とする。あるいは、ライセンスの認証は、アプリケーションが走っているプロセスと同じシステム上で動作するプロセス中のオブジェクトとすることもできる。一旦、第１のオペレーティングシステム上でアプリケーションがインスタンス化されると、オブジェクトプロセスとの通信が必要であると判断される。その結果、その第１のシステム上のカーネルは、ソケットを生成し(６)、適切なヘッダー、マシンアドレス、ポート番号及びプロトコル識別子を含む通信パケットを形成し(８)、その下でアプリケーションが走っているプロセスのクリアランスを維持するデータと秘密度ラベルを添付し(１０)、ソケットを通して、選択された電子通信媒体上でデータパケットを送信する(１２)。

【００２２】インターネットプロトコル(IP)ヘッダーは、通常システムに対する発信元システム情報を含み、該システムは通信と宛先システムに関する情報を発生させる。この情報は、発信元と宛先のコンピュータのマシン番号、該当するアプリケーションと提供されるサービスを識別するポート番号またはアドレス、及び２台のコンピュータが通信するプロトコル(例えば、TCP/IPまたはUDP/IP)を含む。ポート番号またはアドレスは、クライアントのコンピュータ上を走るアプリケーションまたはサブジェクト、及びリモートマシン１３またはサーバー上のライセンス認証プログラムのような宛先マシン上でアクセスされるアプリケーションのオブジェクトまたは資源を識別する。

【００２３】ネットワーク通信中は、IPヘッダーとデータが発信元システムからソケット端点を通して、宛先サーバーによる受け取り(１８)のために電子的に通信される(１４)。宛先のカーネルは、要求されたポートが利用できるかどうかを判断する(２０)。ポートの利用ができ

る(つまり、未だ開かれていない)場合は、着信の秘密度ラベルに関連付けられたクリアランスレベルで、要求されたポートが開かれる(２２)。要求されたポート番号が使用中であれば、その要求は、例えば発信元サーバーに返信される否定応答(NACK)によって却下される(３２)。アクセス制御セキュリティ機構の下にある発信元システムと宛先システムの間の双方向通信に対しても同じ分類レベルが要求される。

【００２４】要求が処理されると、宛先システムは、ポートを開き(２２)、回答のために応答とIPヘッダーを用意する(１６)。目的のアプリケーションを走らせているプロセスのIP秘密度ラベルが、応答に添付される(２８)。強制アクセス制御の下では、秘密度ラベルは、元のシステムの要求と同じセキュリティ分類を含まなければならない。返信パケットは、さらに発信元サーバーに送信され(２０)、そこではパケットが発信元カーネルによって捕捉され(２９)、そのシステムのセキュリティプロトコルにしたがって点検される(３０)。もし返信パケットが、元の要求と同じセキュリティレベルと同じレベルに用意されていなければ、そのパケットは却下される(３２)。そうでなければ、パケットは要求側アプリケーションに送信される(３４)。

【００２５】図３は、同時に実行されている同じ選択アプリケーション４０の第１から第４のインスタンスを含む先行技術によるマルチレベル信頼システムを示している。実行アプリケーションのアプリケーションインスタンスは、それぞれプロセス４２ａ～４２ｄである。プロセス４２ａ～４２ｄのそれぞれは、特定のセキュリティ分類を与えられ、各プロセスは、アプリケーション４０とカーネル４４の間の通信を取扱う。与えられたセキュリティ分類は、ユーザーまたはカテゴリーの識別記号に基づく所定のクリアランスレベル、または例えばアプリケーションのタイプとすることができる。カーネル４４は、実行アプリケーション４０の入出力機能、メモリー、プロセス及び操作の領域を制御する。カーネル４４は、アプリケーション４０のプロセスと、オブジェクト、サービス及びアプリケーション４０のプロセスに接続する外部のアプリケーションのような、選択された資源４８の間の関係を仲介する(４６)。カーネル４４は、アプリケーション４０の各プロセスが、所定のセキュリティポリシーと一致するセキュリティ分類を持つ資源のみと通信するようにする、セキュリティプロセス５０を含む。例えば、強制アクセス制御手順(MAC)システムにより、セキュリティプロセス５０は、プロセス４２ａ～４２ｄのみが、アプリケーション４０の相当するプロセスと同じセキュリティ分類の資源４８のみと通信するようにする。MACの対象はすべて、アプリケーションのプロセスと、それがメッセージの交信を行なう資源の間を行き来する通信パケットに使われるセキュリティラベルによって然るべくラベル付けされる。

【００２６】図４は、本発明によるマルチユーザー、マルチレベル発信元信頼コンピュータシステムで、インターネットのような通信ネットワーク５５を介して第２のコンピュータにネットワークされるものを示す。通常の構成においては、いくつかのユーザーが一つのサーバーにネットワークされる。発信元信頼コンピュータシステム５０は、複数のユーザーワークステーション５６ａ～５６ｄ、サーバー５８、及び発信元信頼コンピュータシステム５０への不当なアクセスを防止する防火壁として採用されるゲートウェイサーバー６０を含むネットワークを有する。ゲートウェイサーバー６０は、カーネル(図示されない)を格納するメモリー６１を含む。第２のコンピュータシステム５４は、カーネルを格納するメモリー６２を有する。受信メッセージに対しては、ゲートウェイサーバー６０のカーネル(図示しない)により受信パケットのセキュリティ検査が行われる。受信パケットは、そのパケットが発信元信頼コンピュータシステム６０のセキュリティプロトコルを満足したことが確定した後にのみ発信元信頼コンピュータシステム５０に通される。例えば、強制的アクセス制御セキュリティプロトコルを使うマルチレベル信頼システムにおいては、発信元信頼コンピュータシステム５０のカーネルは、受信通信パケットの秘密度ラベルが宛先プロセスまたは、そのパケットが仕向けられているコンピュータシステム５４のポートの宛先と同じかそれより高くなるようにする。パケットセキュリティ分類がセキュリティ分類宛先ポートと同じかそれより高くない場合は、そのパケットに対してはそれ以上のプロセスは行われない。メッセージパケットは、モデム６４またはネットワークインターフェースカードを介して、銅線を使った選択された送信媒体６２、光ファイバーリンク、マイクロウェーブ回線またはラジオ放送送信リンク上を送信される。宛先コンピュータシステム５４との選択されたリンクは、LAN接続、直接電話リンクを使って直接に、またはインターネットを介するように間接的に行われる。宛先コンピュータシステムサーバーに到着すると、メッセージパケットは、サーバーのカーネル(図示しない)によって停止される。宛先サーバーがOSIインターフェースを採用している場合は、メッセージはOSI層の最低のソフトウェアレベルで好適に分析され、カーネルが各メッセージパケットを点検するようにする。

【００２７】ある実施例においては、各ワークステーション８６は、モデム６４を介してインターネット５５と接続し、またセキュリティを履行するカーネルを含む。

【００２８】図５は、要求アプリケーションが第１のデータ処理ノード４５(すなわちマシン１)上で走る、本発明によるマルチレベルポートを構成するための方法のフロー図である。第２のデータ処理ノード８６(すなわちマシン２)は、所定のセキュリティ分類に関連付けられた複数のポートを含む。本発明によれば、マシン１は、

選択されたアプリケーションを実行し(６８)、ユーザーのセキュリティクリアランスと一致するそれ自身のセキュリティレベルを確立する。実行アプリケーションが他のデータ処理ノードで資源またはオブジェクトを要求すると、ローカルのマシンカーネルは、サービス要求を運ぶメッセージを作成することができる他の資源またはオブジェクトへのソケットを開放する(７０)。ソケットは、宛先マシン、実行中のアプリケーションプログラムに相応するポート番号、及びローカルのプロセスセキュリティレベルを確認する。ポートの識別子は、カーネルによって開かれた関連するポート番号のための該当するセキュリティレベルを最初に要求することによって生成される(７２)。カーネルはさらに、要求されたポートがそのセキュリティレベルで利用できるかどうかを知るためのチェックを行なう(７４)。もしそのポート番号とセキュリティレベルの組み合わせが、現在使用中(たとえば、他のユーザーにより)であれば、カーネルは所定時間待機した後(７６)、再度ポーリングして、特定のセキュリティレベルがそのポート番号で利用できるかどうかを判断する。他方、もし特定のポート番号とセキュリティ分類の組み合わせが利用できるものである場合は、カーネルはそのセキュリティレベルとポート番号を組み合わせて、ポート識別子を生成する(７８)。次に、ポート番号と秘密度ラベルの組み合わせを、通常はポート番号のみに予約されているIPヘッダーのプロトコルのスペースに挿入することによって、メッセージパケットに対する該当するIPヘッダーが生成される(８０)。メッセージパケットは、アプリケーションに特有なデータと情報をIPヘッダーの所定の場所に添付し(８２)、完全なデータグラムを生成することによって完成される。完成されたデータグラムパケットは、次に電子的通信用にフォーマットされ84、宛先サーバー86に送られる。

【００２９】データ処理ノード８６のオペレーティングシステムのカーネルは、マシン１からのパケットを捕捉し(８８)、ポート識別子を抽出するためにパケットのサブエレメントを検査する(９０)。ポート番号とセキュリティラベルが抽出された後は、カーネルは、指定されたセキュリティレベルで要求されたポートが解放状態にあるかどうかを調べ、もしそうであれば、現在アクセスが可能かどうかを調べる(９２)。もしポート番号と秘密度ラベルの組み合わせが他のアプリケーションによって使用されているため利用できない場合は、そのオペレーションは終了する(９３)。もしポートが利用できる状態であれば、メッセージパケットからの該当するデータは、データ処理ノード８６の該当するオペレーティングシステムのスタックのアプリケーションの部分に移送され(９４)、アプリケーションが処理される。アプリケーションに対してデータが作成された後は、該当する応答が適宜作成され(９６)、該当するIPヘッダーが、作成された応答メッセージに添付される(９８)。応答メッセージは、電子ネットワーク上でのパケット送信用にフォーマットされ(１００)、第１のデータ処理ノード４５に送られる。

【００３０】第１のデータ処理ノード４５のカーネルは、該当する応答パケットを捕捉し(１０２)、パケットを点検して、応答メッセージが、データ処理ノード４５で実行されている該当するアプリケーションの処理と同じセキュリティレベルで作成されたものであるかを確認する(１０４)。ローカルのプロセスと受信されたリモートメッセージのセキュリティレベルが同一であれば、応答はアプリケーションに送られ、処理される(１０６)。応答が該当するローカルのアプリケーションのセキュリティレベルと一致しないセキュリティレベルにある場合は、応答パケットは終了され、また、もし実施可能であれば、否定応答が第２のデータ処理ノード８６に送られる(１０８)。図５に示す応答パケットの検査は、応答パケットのセキュリティレベルが該当するプロセスのセキュリティレベルと同じか同等であることを示すが、本発明によれば、応答パケットがアプリケーションによって読まれるためには、該応答パケットは低位のセキュリティレベルでよい。いかなるアクセス制御でも、その制御がシステムのセキュリティポリシーと一致している限り、メッセージパケットの受け取り取りに使用できる。

【００３１】図６は、要求されたポートがデータ処理ノード間の通信に利用できるかどうかを判断する本発明による方法を示す。特に、受信するパケット８６ｉが宛先システムのオペレーティングシステムによって捕捉されること(１１０)を示している。セキュリティの検査は、カーネルインターフェースオペレーティングシステムのインターフェース６６のデータリンク層とネットワーク層のレベルで行われる。パケット８６ｉのIPヘッダーエレメント１１２がチェックされ、ポート番号と秘密度ラベルサブエレメント１１４が確認される。カーネルは、要求されたポート番号が既に解放されているかどうかの判断のためのチェックを行う(１１６)。もし開放されていなければ、要求されたポートは、秘密度ラベルで示されたセキュリティレベルで開放される(１１８)。特定のセキュリティレベルでポートを開く挙動は、その挙動の日誌または履歴を作成し、また特定のポート番号に対して現在開かれているセキュリティレベルのデータベースを作成するために記録される(１２２)。パケットをローカルのアプリケーションに渡すかどうかの判断が行われる(１２０)。他のすべてのプロトコルの要件が満たされた場合は、データはその処理、完了のため、アプリケーションプロセス８６''に送られる。もし他のすべてのプロトコル要件が満足されなければ、パケットは破棄される(１０８)。

【００３２】要求された登録済みポート番号が既に解放されている場合(１１６)、オペレーティングシステムのカーネルは、それぞれの解放されたポートがポート識別

子のセキュリティラベルで指定されたセキュリティレベルにあるかどうかを判断する(１２４)。そしてそのレベルにない場合は、既存のポートと同一番号を持つ新しいポートが、そのセキュリティレベルで開放される(１１８)。ポートの解放は、上述のようにその挙動として記録される(１２２)。そして既存の解放されたポートがポート識別サブエレメント中で識別されたものと同一のセキュリティレベルである場合、そのポートが使われているかどうかが判断される(１２６)。そしてもしポートが現在使用中であれば、強制的アクセス制御プロトコルが、開放されているものと同じ番号及びセキュリティレベルの他のポートの解放を阻止する。その結果、パケットは、所定のタイムアウトが発生し(１３０)、パケットプロセス終了が発生するか、あるいはパケットが直ちに終了する(１０８)まで、あるいはポートが使用されなくなる(１２４)まで、バッファに入れられ(１２８)且つ定期的にチェックされる。解放されたポートが正しいセキュリティレベルにセットされているが、現在使用されていない場合(１２６)は、ポートの活動が記録され、またパケットを通過させるかどうかの判断がなされる(１２０)。他のすべてのセキュリティ基準が満足されていれば、パケットはアプリケーション処理のため渡される。

【００３３】本発明によれば、選択アクセス制御セキュリティ機構に依拠したオペレーティングシステムを持つコンピュータシステムは、セキュリティ分類レベルの階層(たとえば、トップシークレット、シークレット、クラシファイド、非クラシファイド)が定義されている政府のシステム及び商業システムを含む。本出願の目的から、アクセス制御セキュリティ機構による秘密度ラベルは、上述のように、少なくとも階層的セキュリティ分類を含み、また非階層的カテゴリーまたは区画を含んでいてよい。たとえば、これらのカテゴリーは、特定の人口統計、製品の種類並びに、会計、広報、流通、技術及びR&Dのような機能的分類として定義されるカテゴリーに従った各種のプラント工場に当てはめることができる。したがって、特定のセキュリティ分類を持つ実体は、それぞれのカテゴリーにおけるそのレベルのすべての情報に対して自動的に明らかにされるものではない。コンピュータシステムのメモリー内でインスタンス化されるアプリケーションは、同じシステムまたは異なるシステム上の第三者資源またはオブジェクトへのアクセスを要求できる。カーネルは、ユーザーが資源を要求する許可を持っていることを判断した後、その資源との通信の準備の中でIPヘッダーを発生させる。IPヘッダーには、発信元及び宛先のマシン識別番号及びポート識別子が含まれる。宛先システムのポート識別子は、発信元のアプリケーションによって要求される特定の資源、データベースまたはサービスを指定するポート番号、及び秘密度ラベルで構成される。秘密度ラベルは、アプリケーションを実行するプロセスのセキュリティ分類またはクリアランスを含み、またカテゴリー制限のような他の情報を含むこともできる。発信元システムのカーネルは、データグラムまたはメッセージパケットを生成するために、ヘッダーに対していかなるアプリケーションデータでも添付することができる。発信元システムのカーネルはさらに、通信ソケットを開き、また結果として得られるパケットを選択された宛先システムに送信する。

【００３４】宛先システムのカーネルは、送られたパケットを受け取り、パケットヘッダー内のポート識別子を分析する。要求されたポート番号が宛先システム上で未だ開かれていない場合は、宛先システムのカーネルは、パケットヘッダー(すなわち、同じまたは低位の分類レベル)内のポート識別子の中の秘密度ラベルによって識別されたセキュリティレベルと一致するプロセスセキュリティレベルで、要求されたアプリケーションを起動する。処理の実行は、発信元のシステムパケットの秘密度ラベルを付帯したカテゴリー指定方法によってさらに修正され、同一ポート番号で多数のポートを確立し、更に異なるカテゴリーに対するクリアランスを確立することができる。パケットの検査と読み取りは、宛先システムのサーバー、宛先サーバーと第三者システムの間の防火壁の役目をするゲートウェイ、または宛先サーバーと互いにネットワークされたすべてのサーバーにおいて、本発明による一実施例によって行われる。

【００３５】さらに本発明によれば、すべての要求ジョブ及びサービスが行われる。目的のプロセスのクリアランスが発信元プロセスのクリアランスと同一であれば、宛先システムのカーネルは、発信元のコンピュータシステムへの送信のための応答パケットを生成する。しかしながら、宛先システムのカーネルがポート番号は解放されているが、発信元と関連付けられた秘密度ラベルが解放されたポートの秘密度ラベルと異なると判断した場合は、宛先システムのカーネルは、発信元のポートの識別子の秘密度ラベルと一致するセキュリティ分類における同じポート番号を持つ他のポートを開く。同様に、そのIPヘッダー内に発信元のポートの識別子を持つ別の受信パケットが、第３の、異なるセキュリティ分類における宛先ポートの第３のインスタンスの解放を要求する場合は、宛先システムのカーネルは、第３のポートの識別子の秘密度ラベルと一致するセキュリティ分類を持つプロセスによるアプリケーションの第３のインスタンスを開始する。同じポート番号を持つアプリケーションのインスタンスの数は、分類レベルの数と同じだけ解放または同時に走らせることができることが明らかである。さらに、固有のポート識別子を生成するために別のカテゴリーを使った場合は、同時に解放できる共通のポート番号を持つポートの数は、カテゴリーの数の合計となる。

【００３６】宛先システムのカーネルが、特定の分類レベルで、または同一カテゴリに対してポート番号が解放されていると判断し、それが解放されている場合は、宛

先システムのカーネルは、受け取ったパケットを開かれた宛先プロセスに引き渡す。しかしながら、宛先ポートが適切な分類レベルを持っているか、同一カテゴリーが前に受け取った要求で現在塞がれている場合は、宛先システムのカーネルは、受け取ったパケットを関連する宛先プロセスに引き渡さない。その代わり、受け取り側のカーネルは、受け取ったパケットを、プロセスが受け入れできるセキュリティレベルで利用できるようになるまでバッファに保持、またはパケットを拒否することができる。そして適切な応答メッセージを元システムに送り返すことができる。

【００３７】例としてあげるとすれば、制限なしに、コンピュータのオペレーティングシステム内でインスタンス化されたアプリケーションは、ライセンスの確認、認証のために外部資源へのアクセスを要求することができる。その結果、受け取り側のシステムのオペレーティングシステムは、発信元及び宛先のソケットの識別子と通信プロトコルを含むIPヘッダーで構成されるデータグラムまたはメッセージパケットを構成し、またアプリケーションに関連するライセンス認証要求を添付できる。発信元のプロセスに関連付けられたソケットは、マシンアドレスと、希望する資源(たとえばライセンス確認サービス)を識別するポート番号を含む。本発明によれば、新しいポート識別子は、ポート番号と秘密度ラベルで構成される。受け取り側ライセンスサーバーによってメッセージデータグラムまたはパケットを受け取ったとき、受け取り側のカーネルは、受信メッセージを受け取り側システムのセキュリティプロトコルによって検証する。受け取り側のカーネルは、メッセージヘッダー内の秘密度ラベルによって指示された特定の分類において、受信メッセージによって指定されたポートが解放されているかどうかを判断する。その分類でポートが解放されていないか使用されていない場合は、カーネルは受信メッセージパケットを通信マネージャーに移送し、表示された秘密度ラベルでのプロセスでインスタンス化されたライセンス確認アプリケーションを開く。指定されたセキュリティ分類でのポートが既に開かれており、使用中であれば(即ち、要求された資源が、同一セキュリティ分類で他のユーザーによって使われている)、そのパケットはバッファに入れられまたは破棄され、否定応答を発信元システムに返送することができる。

【００３８】本発明によれば、受け取り側システム内にあるセキュリティデーモン(daemon：事象駆動型プログラム守護機能)が受け取りシステムのセキュリティプロトコルを実行し、到着するメッセージパケットを受け取

るかどうか、また要求されたセキュリティレベルでポートを開くかどうかを判断する。本発明の一つの実施例によるセキュリティデーモンは、開かれたシステムの相互接続(OSI)データリンク層とOSIネットワーク層の間で活動する。受信データグラムとパケットメッセージを点検することにより、セキュリティデーモンは、カーネルが、ローカルのインターフェースを行き来するパケットとメッセージを確実に捕捉し、点検するようにさせる。本発明によるセキュリティデーモンは、ポート識別子の個々のパケットエレメントとサブエレメントにアクセスする。

【００３９】本発明によれば、同一ポート番号と固有の秘密度ラベルを持つ多重システムソケットまたは端点は、マルチレベル信頼システムを含むネットワークの端点におけるサードパーティアプリケーションに解放される。

【００４０】本発明は、ここでは実施例に基づいて説明しているが、上述の説明を読めば、当業者にとっては、各種の代替方法があることが明らかになるはずである。たとえば、秘密度ラベルは発信元サーバーにおけるポート番号に関連付けられる必要はない。ポート番号と秘密度ラベルの両方で構成される、本発明による合成されたポート識別子は、破壊ポートを解放する前にいつでも構築できる。したがって、発信元データ処理におけるソフトウェアの修正は、秘密度ラベルをポート番号と組み合わせること含む必要はない。ポート番号は、送達パケット中のデータと関連付けたり、宛先サーバーのカーネルによる検証に付随するポート番号と組み合わせることもできる。

【図面の簡単な説明】

【図１】所定のセキュリティレベルの複数のポートと端点を持つ先行技術によるマルチレベル信頼システムのブロック図である。

【図２】データグラムまたはメッセージパケットが発信元システムと宛先システムの間で交信される先行技術によるマルチレベル信頼システムのフロー図である。

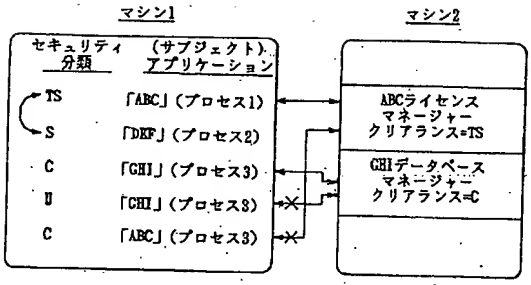
【図３】先行技術によるセキュリティシステムのブロック図である。

【図４】本発明によるインターネットシステムの図である。

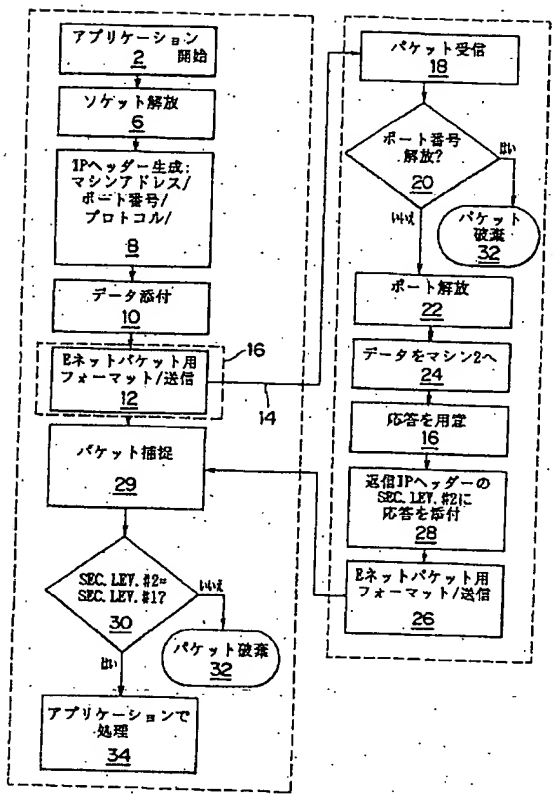
【図５】本発明によるマルチレベル信頼システムのフロー図である。

【図６】本発明による通信パケットを処理するマルチレベル信頼システムの図である。

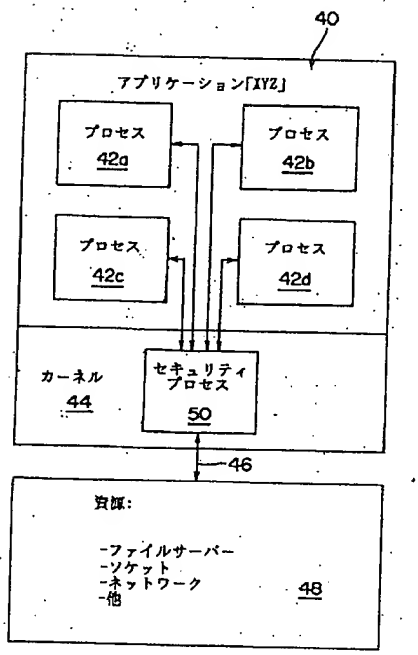
【図１】


マシン1
マシン2
セキュリティ分類
(サブジェクト)アプリケーション
TS
S
C
U
C
「ABC」(プロセス1)
「DEF」(プロセス2)
「GHI」(プロセス3)
「CHI」(プロセス8)
「ABC」(プロセス8)
ABCライセンスマネージャー
クリアランス=TS
CHIデータベースマネージャー
クリアランス=C

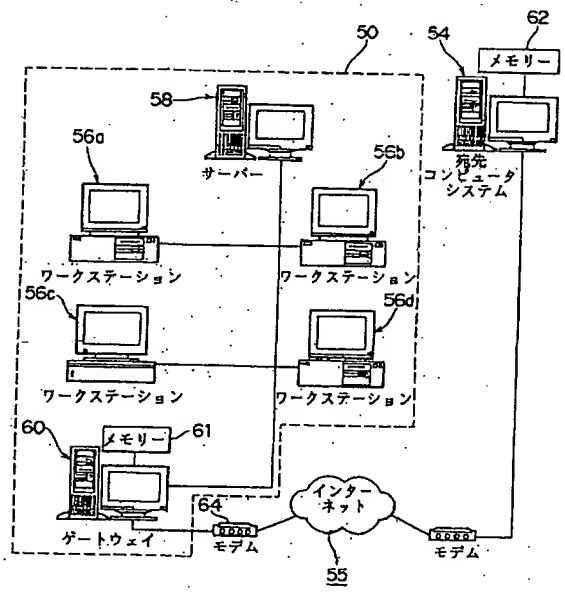
【図２】


アプリケーション 2 開始
ソケット解放 6
IPヘッダー生成;マシンアドレス/ポート番号/プロトコル/ 8
データ添付 10
Eネットパケット用フォーマット/送信 12
16
14
パケット捕捉 29
SEC. LEV. #2= SEC. LEV. #1? 30
いいえ
はい
パケット破棄 32
アプリケーションで処理 34
パケット受信 18
ポート番号解放? 20
はい
いいえ
パケット破棄 32
ポート解放 22
データをマシン2へ 24
応答を用意 16
返信IPヘッダーのSEC. LEV. #2に応答を添付 28
Eネットパケット用フォーマット/送信 26

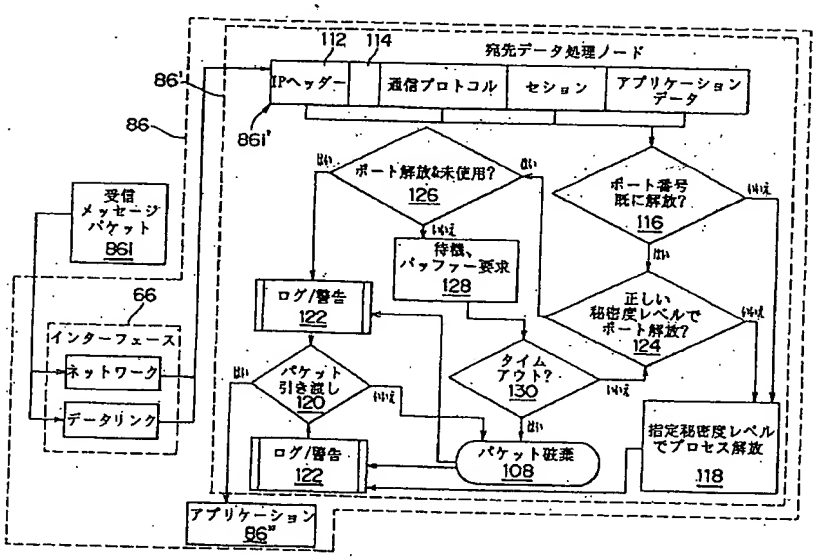
【図３】


40
アプリケーション「XYZ」
プロセス 42a
プロセス 42b
プロセス 42c
プロセス 42d
カーネル 44
セキュリティプロセス 50
46
資源:
-ファイルサーバー
-ソケット
-ネットワーク
-他
48

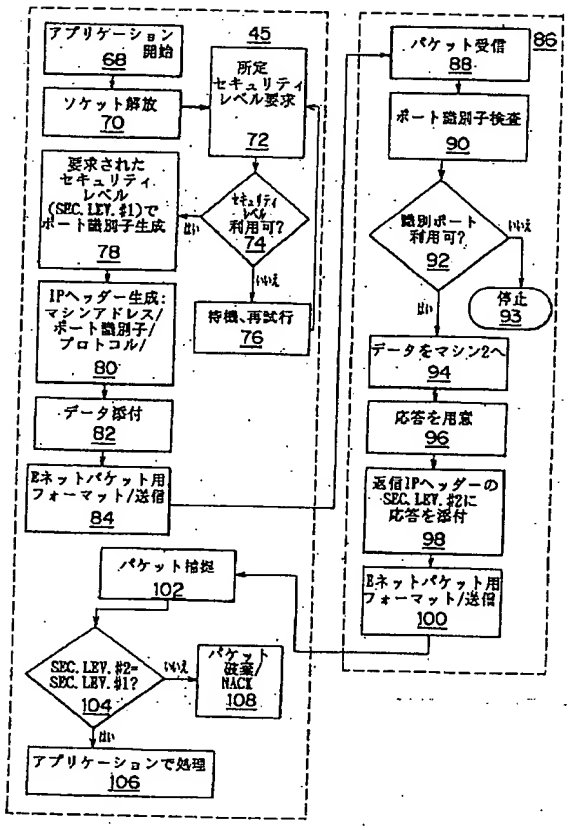
【図４】


50
54
62
メモリー
58
サーバー
56a
56b
宛先
コンピュータ
システム
ワークステーション
ワークステーション
56c
56d
ワークステーション
ワークステーション
60
メモリー
61
64
インター
ネット
ゲートウェイ
モデム
モデム
55

【図６】


宛先データ処理ノード
112
114
IPヘッダー
通信プロトコル
セション
アプリケーション
データ
86'
86
ポート解放&未使用?
126
ポート番号
既に解放?
116
待機、
バッファー要求
128
正しい
秘密度レベルで
ポート解放?
124
ログ/警告
122
タイム
アウト?
130
パケット
引き渡し
120
パケット破棄
108
指定秘密度レベル
でプロセス解放
118
ログ/警告
122
受信
メッセージ
パケット
86i
66
インターフェース
ネットワーク
データリンク
アプリケーション
86"

【図５】



フロントページの続き

(51) Int.Cl.[6]	識別記号	FI	
H04L 12/56		H04L 11/20	102Z

(71)出願人　591064003
901 SAN ANTONIO ROAD
PALO ALTO, CA 94303, U.
S. A.